Claims:

1. A method of mitigating a Denial of Service (DOS) attack on a first node in a computer-based communications network comprising the steps of:

a) detecting at a second node located upstream of the first node a traffic pattern indicating a possible DOS attack on the first node;
b) sending from the second node to the first node a notification of the possible attack; and
c) implementing, at the second node, attack mitigation measures to mitigate the attack on the first node.

2. The method as defined in claim 1 wherein the second node awaits input from the first node before implementing an attack mitigation measure.

3. A method of mitigating a Denial of Service (DOS) attack on a first node in a computer-based communications network comprising the steps of:

a) detecting at a second node located upstream of the first node a traffic pattern indicating a possible DOS attack on the first node;
b) sending from the second node to the first node a notification of the possible attack;
c) receiving at the first node the notification and determining whether attack mitigating measures should be implemented;
d) if attack mitigation measures are to be implemented sending from the first node instruction to the second node to implement the measures; and
e) implementing the attack mitigation measures at the second node.

4. The method as defined in claim 3 wherein the notification from the second node includes a random nonce or other authentication information with which to verify the response of the first node.

5. The method as defined in claim 3 wherein the notification from the second node includes a suggested attack mitigating measure.

6. The method as defined in claim 3 wherein -the response from the first node to the second node includes an attack mitigating measure.

7. The method as defined in claim 6 wherein the response from the first node to the second node includes a duration of implementation of the mitigating measure.

8. The method as defined in claim 3 wherein the second node analyzes traffic passing through it to detect traffic patterns that indicate a possible DoS attack.

9. The method as defined in claim 8 wherein the second node examines resource usage for its output ports to detect traffic patterns that indicate a possible DOS attack.

10. The method as defined in claim 3 wherein the first node determines whether an attack mitigation measure should be implemented by scanning its input ports for required resources and if they are excessive instructing the second node to implement the measure.

11. The method as defined in claim 10 wherein the type of measure implemented by the second node is based on the nature of the DOS attack.

12. A system for mitigating a Denial of Service (DOS) attack on a first node in a computer-based communications network comprising:

a second node located upstream of the first node for detecting a traffic pattern indicating a possible DOS attack on the first node;

means for sending from the second node to the first node a notification of the possible attack; and

means in the second node to implement an attack mitigation measure to mitigate a DOS attack on the first node.

13. The system as defined in claim 12 wherein the second node includes means to receive instructions from the first node regarding an attack mitigation measure.

14. A system for mitigating a Denial of Service (DOS) attack on a first node in a computer-based communications network comprising:

means in the first node for receiving information from a second node located upstream of the first node indicating a possible DOS attack on the first node;

means in the first node for determining whether the information is valid; and

means for responding to the second node.

15. The system as defined in claim 14 wherein the first node provides information regarding an attack mitigating measure.